What is claimed is:

1. A bit error resilience method for an Internet Protocol (IP) stack based on a secure link layer having functionality for packet error detection, said method comprising the steps of:

- analyzing packets at said secure link layer to determine whether the packets are header compressed; and

- forwarding at least header compressed packets with detected errors at said link layer upwards in the protocol stack for higher-level error protection.

2. The bit error resilience method according to claim 1, wherein said higher-level error protection includes subpacket error detection.

3. The bit error resilience method according to claim 1, wherein said higher-level error protection includes error correction.

4. The bit error resilience method according to claim 1, wherein all header compressed packets are forwarded upwards in said protocol stack for higher-level error protection.

5. The bit error resilience method according to claim 1, wherein said higher-level error protection includes the step of protecting header information in said header compressed packets on a higher sublevel of said link layer.

6. The bit error resilience method according to claim 5, wherein said higher sublevel is the Header Compression (HC) level.

7. The bit error resilience method according claim 1, wherein said higher-level error protection includes the step of protecting header information and at least part of the payload in said packets on the User Datagram Protocol (UDP) level.

8. The bit error resilience method according to claim 1, wherein said higher-level error protection includes the step of protecting at least part of the payload in said packets on the application level.

9. The bit error resilience method according to claim 7 or 8, wherein said packets include compressed real-time data such as compressed voice or video, and said higher-level error protection of at least part of the payload includes the step of protecting critical real-time parameters in the payload.

10. The bit error resilience method according to claim 5, wherein said step of protecting header information in said header compressed packets includes the step of protecting at least part of the compressed header by a local checksum, which is selected as a local subset of said compressed header.

11. The bit error resilience method according to claim 10, wherein said local checksum is a predetermined portion of a Context Identifier (CID) field in said compressed header.

12. The bit error resilience method according to claim 10, wherein said local checksum is a predetermined portion of a Generation field in said compressed header.

13. The bit error resilience method according to claim 10, wherein said local checksum is a predetermined portion of an IPv4 identifier field in said compressed header.

14. The bit error resilience method according to claim 10, wherein said protected compressed header information includes said local checksum.

15. The bit error resilience method according to claim 1, wherein said header compressed packets are header compressed according to one of the following standards:

- RFC 2507 of the Internet Engineering Task Force (IETF);
- RFC 2508 of the IETF; and
- Robust checksum-based header compression (ROCCO) of the IETF.

16. The bit error resilience method according to claim 10 or 11, wherein said header compressed packets are header compressed according to one of the following standards:

- RFC 2507 of the Internet Engineering Task Force (IETF);
- RFC 2508 of the IETF; and
- Robust checksum-based header compression (ROCCO) of the IETF.

17. The bit error resilience method according to claim 1, further comprising the step of discarding a header compressed packet with a faulty link layer checksum if the indicator of a dynamic Delta value for an Internet Protocol version 4 (IPv4) identifier is set.

18. The bit error resilience method according to claim 1, further comprising the step of discarding full header packets with faulty link layer checksums.

19. The bit error resilience method according to claim 1, further comprising the step of discarding full header packets with faulty IPv4 checksums, thus protecting from bit error propagation on the Internet Protocol (IP) level.

20. The bit error resilience method according to claim 1, wherein the framing protocol of said secure link layer is the Point-to-Point Protocol (PPP).

21. The bit error resilience method according to claim 1, wherein said secure link layer is the High-level Data Link Control (HDLC) protocol layer.

22. A method for protecting header information in header compressed packets, comprising the steps of:

- selecting a first subset of the compressed header as a local checksum; and
- protecting a second subset of said compressed header by said selected local checksum.

23. The method according to claim 22, wherein said local checksum is a predetermined portion of a Context Identifier (CID) field in said compressed header.

24. The method according to claim 22, wherein said local checksum is a predetermined portion of a Generation field in said compressed header.

25. The method according to claim 22, wherein said local checksum is a predetermined portion of an IPv4 identifier field in said compressed header.

26. The method according to claim 22, wherein said compressed header is a combination of at least part of a Point-to-Point Protocol (PPP) header and a Header Compression (HC) header.

27. The method according to claim 22, wherein said protected second subset of said compressed header includes said local checksum.

28. The method according to claim 22 or 23, wherein said header compressed packets are header compressed according to one of the following standards:

- RFC 2507 of the Internet Engineering Task Force (IETF);
- RFC 2508 of the IETF; and
- Robust checksum-based header compression (ROCCO) of the IETF.

29. A bit error resilience system for an Internet Protocol (IP) stack based on a secure link layer having means for checksum error evaluation, said system comprising:

- means for analyzing packets at said secure link layer to determine whether the packets are header compressed; and
- means for forwarding at least header compressed packets with faulty link layer checksums upwards in said protocol stack for higher-level error protection.

30. The bit error resilience system according to claim 29, wherein said higher-level error protection includes subpacket error detection.

31. The bit error resilience method according to claim 29, wherein said higher-level error protection includes error correction.

32. The bit error resilience system according to claim 29, wherein said forwarding means is operative for forwarding all header compressed packets upwards in the protocol stack for higher-level error protection.

33. The bit error resilience system according to claim 29, wherein said higher-level error protection is effectuated at least partly by means for protecting header information in said header compressed packets on a higher sublevel of said link layer.

34. The bit error resilience system according to claim 33, wherein said higher sublevel is the Header Compression (HC) level.

35. The bit error resilience system according to claim 29, wherein said higher-level error protection is effectuated at least partly by means for protecting header information and at least part of the payload in said packets on the User Datagram Protocol (UDP) level.

36. The bit error resilience system according to claim 29, wherein said higher-level error protection is effectuated at least partly by means for protecting at least part of the payload in said packets on the application level.

37. The bit error resilience system according to claim 35 or 36, wherein said packets include compressed real-time data such as compressed voice or video, and said higher-level error protection of at least part of the payload is effectuated by means for protecting critical real-time parameters in the payload.

38. The bit error resilience system according to claim 33, wherein said means for protecting header information in said header compressed packets includes means for protecting at least part of the compressed header by a local checksum, which is selected as a local subset of said compressed header.

39. The bit error resilience system according to claim 38, wherein said local checksum is a predetermined portion of a Context Identifier (CID) field in said compressed header.

40. The bit error resilience system according to claim 38, wherein said local checksum is a predetermined portion of a Generation field in said compressed header.

41. The bit error resilience system according to claim 38, wherein said local checksum is a predetermined portion of an IPv4 identifier field in said compressed header.

42. The bit error resilience system according to claim 38, wherein said protected compressed header information includes said local checksum.

43. The bit error resilience system according to claim 29, wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

44. The bit error resilience system according to claim 38 or 39, wherein said header compressed packets are header compressed according to one of the following standards:

RFC 2507 of the Internet Engineering Task Force (IETF);

RFC 2508 of the IETF; and

Robust checksum-based header compression (ROCCO) of the IETF.

45. The bit error resilience system according to claim 29, further comprising means for discarding a header compressed packet with a faulty link layer checksum if the indicator of a dynamic Delta value for an Internet Protocol version 4 (IPv4) identifier is set.

46. The bit error resilience system according to claim 29, further comprising means for discarding full header packets with faulty link layer checksums.

47. The bit error resilience system according to claim 29, further comprising means for discarding full header packets with faulty IPv4 checksums, thus protecting from bit error propagation on the Internet Protocol (IP) level.

48. The bit error resilience system according to claim 29, wherein the framing protocol of said secure link layer is the Point-to-Point Protocol (PPP).

49. The bit error resilience system according to claim 29, wherein said secure link layer is the High-level Data Link Control (HDLC) protocol layer.

50. A system for protecting header information in header compressed packets, said system comprising:

- means for selecting a first subset of the compressed header as a local checksum; and
- means for protecting a second subset of said compressed header by said selected local checksum.

51. The system according to claim 50, wherein said local checksum is a predetermined portion of a Context Identifier (CID) field in said compressed header.

52. The system according to claim 50, wherein said local checksum is a predetermined portion of a Generation field in said compressed header.

53. The system according to claim 50, wherein said local checksum is a predetermined portion of an IPv4 identifier field in said compressed header.

54. The system according to claim 50, wherein said compressed header is a combination of at least part of a Point-to-Point Protocol (PPP) header and a Header Compression (HC) header.

55. The system according to claim 50, wherein said protected second subset of said compressed header includes said local checksum.

56. The system according to claim 50, wherein said protected second subset of said compressed header comprises static or quasi-static information.

57. The system according to claim 50 or 51, wherein said header compressed packets are header compressed according to one of the following standards:

- RFC 2507 of the Internet Engineering Task Force (IETF);
- RFC 2508 of the IETF; and
- Robust checksum-based header compression (ROCCO) of the IETF.